UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. APPROXIMATELY 1,435,014.299980 TETHER, Defendant.	)	Case No. 12-cv-12576 Judge

VERIFIED COMPLAINT FOR CIVIL FORFEITURE *IN REM*

The United States of America, by MORRIS PASQUAL, Acting United States Attorney for the Northern District of Illinois, for its verified complaint against the above-named defendant properties and in accordance with Supplemental Rule G(2) of the Federal Rules of Civil Procedure alleges as follows:

NATURE OF THE ACTION

1. This is a civil action brought by 18 U.S.C. §§ 981(a)(1)(A) and 981(a)(1)(C) for forfeiture *in rem* of the defendant property. The United States seeks forfeiture of the properties described in paragraph three (3) below, which constitute proceeds, or property traceable to proceeds, of a wire fraud offense or offenses committed in violation of 18 U.S.C. § 1343 and were involved in the commission of a money laundering offense or offenses committed in violation of 18 U.S.C. § 1956. In addition, under 18 U.S.C. § 981(a)(1)(C), with cross references to 18 U.S.C. §§ 1956(c)(7) and 1961(1), "[a]ny property, real or personal, which constitutes or is derived from proceeds traceable to a violation of" fraud are subject to civil forfeiture to the United States.

2. This complaint is verified by the attached Verification of Federal Bureau of Investigation Special Agent Jayna Kadel ("SA Kadel"), which is fully incorporated herein.

THE DEFENDANT PROPERTY

3. The Defendant *in rem* consists of approximately 1,435,014.299980 Tether ("USDT") formerly held in cryptocurrency accounts identified by the following Tether deposit addresses:

(a) 0x1bdd6956015976209e34e5f47C574A0f2cA9BD87 (Subject Asset #1)

(b) 0x7c214b43350B51B8C2B72c0C2b10b764Fc9774c6 (Subject Asset #2)

(c) 0xcf95f287E2856c34130B9D31859f3b2C29b45d50 (Subject Asset #3)

(d) 0xB8C348f248AD0493Ae2e6640D30ce3986413Af23 (Subject Asset #4)

(e) 0x9404a2CBD5e46B91e814909c49fa071F31C86b7d (Subject Asset #5)

(hereinafter the defendant property or "Subject Assets").

4. The Subject Assets have been seized pursuant to a seizure warrant 24M124, dated February 23, 2024, issued by Magistrate Judge M. David Weisman in the Northern District of Illinois and are in the custody of the Federal Bureau of Investigation.

JURISDICTION AND VENUE

5. This court has jurisdiction over this action pursuant to 28 U.S.C. § 1345 and 28 U.S.C. § 1355(a).

6. Venue is proper in this district pursuant to 28 U.S.C. § 1355(b)(1) because the acts or omissions giving rise to the forfeiture occurred at least in part within this district.

BASIS FOR FORFEITURE

7. The defendant property is subject to forfeiture under 18 U.S.C. § 981(a)(1)(C) because it constitutes or was derived from proceeds traceable to an offense constituting "specified unlawful activity" – as defined in 18 U.S.C. § 1956(c)(7), with reference to 18 U.S.C. § 1961(1) – namely, wire fraud, committed in violation of 18 U.S.C. § 1343.

8. The defendant property is also subject to forfeiture under 18 U.S.C. § 981(a)(1)(A) because it was involved in, or is traceable to funds involved in, money laundering transactions in violation of 18 U.S.C. § 1956.

BACKGROUND ON CRYPTOCURRENCY

9. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency

exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[1] Cryptocurrency, itself, it not illegal in the United States.

10. Bitcoin[2] ("BTC") is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people.

11. Ether ("ETH") is a cryptocurrency that is open source, public, has a blockchain, and is distributed on a platform that uses "smart contract" technology. The public ledger is the digital trail of the Ethereum blockchain, which allows anyone to track the movement of ETH. Smart contracts allow developers to create markets, store registries of debts, and move funds in accordance with the instructions provided in the contract's code, without any type of middleman or counterparty controlling a desired or politically motivated outcome, all while using the Ethereum blockchain protocol to

[1] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

[2] Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

maintain transparency. Smart contract technology is one of Ethereum's distinguishing characteristics and an important tool for companies or individuals executing trades on the Ethereum blockchain. When engaged, smart contracts automatically execute according to the terms of the contract written into lines of code. A transaction contemplated by a smart contract occurs on the Ethereum blockchain and is both trackable and irreversible.

12. Stablecoins are a type of virtual currency whose value is pegged to a commodity's price (such as gold), to a fiat currency (such as the U.S. dollar), or to a different virtual currency. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives. Some stablecoins are issued (i.e., created or minted) by a central authority (e.g., a company or other entity) that centrally manages the smart contracts and treasury for the stablecoin.

13. Tether ("USDT") is a stablecoin pegged to the U.S. dollar. Tether Limited ("Tether") is the company that manages the smart contracts and treasury (i.e., reserve assets) for USDT. Because Tether manages the smart contracts for USDT, they are able to blacklist some addresses containing USDT. For example, Tether is able to blacklist addresses holding USDT on the Ethereum network, rendering those funds inaccessible to whomever controls the private keys to the blacklisted addresses. In the instant case, at the request of law enforcement, Tether voluntarily froze/blacklisted the addresses associated with the SUBJECT ASSETS and continued to do so until they received the aforementioned warrant.

14. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous. And while it's not completely anonymous, bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

15. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is usually represented as a case-sensitive string of letters and numbers, 26–90 characters long, often depending on the cryptocurrency protocol. Each public address is controlled and/or accessed with the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an

address's private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

16. Although cryptocurrencies such as bitcoin and Ether have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes—for example, as payment for illegal goods and services and to commit money laundering. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track purchases. The value of cryptocurrency is generally much more volatile than that of fiat currencies. As of October 30, 2024, one BTC is worth approximately $72,377.66, one ETH is worth approximately $2,637.77, and one USDT is worth approximately $.9996.[3]

17. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can access the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available

[3] Historical data as reported by Yahoo Finance.

device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code[4] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase).

18. "Exchangers" and "exchanges" are individuals or companies that exchange bitcoin or other cryptocurrencies for other currencies, including U.S. dollars. According to the United States Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.[5] Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). Registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the

[4] A QR code is a matrix barcode that is a machine-readable optical label.
[5] *See* "Application of FinCEN's Regulations to Person Administering, Exchanging, or Using Virtual Currencies," *available at* https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat-currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10% (in contrast to registered and Bank Secrecy Act-compliant exchangers, who may charge fees as low as 1–2%).

19. Some companies offer cryptocurrency wallet services, which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the specific device on which the wallet application was installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency.

20. As referenced above, in this matter, the SUBJECT ASSETS are associated with virtual currency addresses that exist on the Ethereum network. Pursuant to seizure warrant 24M124 issued in the Northern District of Illinois, on March 6, 2024, Tether "burned" or destroyed the addresses that comprised the SUBJECT ASSETS (and by

extension the USDT tokens associated with them). Tether then reissued the equivalent amount of USDT tokens associated with each address and transferred that USDT to a government-controlled wallet.

FACTUAL BACKGROUND

21. The FBI is investigating a fraud scheme wherein the perpetrators pose as employees of Microsoft or Apple and the victim's bank to convince the victim that they are the subject of a hacking incident. The scheme is initiated via a computer dialogue box (or "popup") that indicates the victim's computer is compromised and directs the victim to call Microsoft or Apple for assistance. Typically, the perpetrators convince the victim his/her financial accounts are at risk and that he/she needs to move money from traditional bank accounts to cryptocurrency to keep it safe from the hackers. Once the victim's money is converted to cryptocurrency, the perpetrators arrange for cryptocurrency to be transferred to digital currency wallets the victim does not control and are presumably controlled by the perpetrators and their co-conspirators. The scheme has affected individuals located all over the United States including at least two known victims located in the Northern District of Illinois.

22. In support of the investigation, the FBI was conducting analysis of the currency transfers into an address that received proceeds from a victim located in Evanston, Illinois,[6] address 0x16A69fe4fFCA1Bc32A0EF15F5Ff9629DA313BAa1

[6] Based on interviews with the victim in Evanston, the victim lost between $2 to $3 million in a scheme similar to the one described herein.

(hereinafter 0x16A69f). The FBI conducted reverse blockchain analysis[7] in an attempt to identify the source of the other funds stored in 0x16A69f. During this process, the FBI identified several intermediary private addresses which had also transferred funds into 0x16A69f. Some of those intermediary addresses received funds from addresses traced to crypto exchange Crypto.com. One such private address was 0x3fa26E5539dfef7b4750b26565CFCd60E8556d28 (hereinafter **0x3fa26E**).[8] Through legal process, the FBI obtained subscriber account information from Crypto.com. The subscriber records identified the account holder as a resident of New Jersey, hereinafter referred to as Victim A.

23. Between March 20 and March 23, 2023, law enforcement conducted several interviews of Victim A. Victim A stated in November 2022, he was working on his computing device when he received a popup alert directing him to contact Apple. Victim A called the number provided and spoke to an individual claiming to work for Apple, and later to an individual claiming to work in the fraud department of Victim A's bank (these unidentified individuals are hereinafter referred to as the "scammers"). The scammers convinced Victim A his Social Security Number (SSN) was compromised, loans had been attempted using Victim A's name and SSN, and his financial assets were at risk. The scammers convinced Victim A he needed to take steps to secure his assets. The scammers suggested they use a secure "treasury account" which was purportedly completely independent of Victim A's compromised SSN and would protect his funds

[7] "Reverse blockchain analysis" is a term utilized by SA Kadel to describe the process by which deposits into an address are traced backwards through the blockchain to identify the original source of funds.
[8] As discussed later, this is the address of Victim A's Exodus Wallet.

until a new SSN was issued. Part of the process of transferring funds to this account involved the use of cryptocurrency, which the scammers suggested further separated Victim A's funds from his at-risk SSN. The scammers said the process was safe and arranged by his bank and that all funds would be returned to his original accounts at some later date.

24. According to Victim A, the scammers provided Victim A with a letter purportedly from the United States Federal Reserve, bearing the signature of Jerome Powell. The letter states, in part, that Victim A is "under contract with the Federal Reserve of United States for IDENTITY THEFT with Mr. Kevin Lawson assigned as fraud prevention officer for completing the Re-validation of your bank accounts and financial assets."[9] Law enforcement shared an image of this letter with a contact at the United States Federal Reserve Board, Office of Inspector General, who indicated the letter is not authentic. According to Victim A, the scammers also provided Victim A with a letter purportedly from the bank where Victim A maintained his individual retirement account. The letter states in part, "In regards to the ongoing Identification Theft & Financial Fraud case of [Victim A], Merrill Fraud Prevention department has decided that majority of the funds from his respective Merrill accounts will be liquidated and transferred to his Secure Treasury Account" and "once all his Merrill accounts are completely secured, entire funds will be transferred back at the completion of the case." The letter further states the case is "being investigated by Mr. Kevin Lawson…under

[9] "Kevin Lawson" is the name provided by the individual claiming to work for Victim A's bank. This name was provided to several other victims known to SA Kadel, who also lost money in a similar manner to Victim A. In each case, Lawson purported to work for the victim's financial institution – in one instance, PNC Bank, in another instance, USAA Bank.

the supervision of Federal Trade Commission & Social Security Administration." Based on my training and experience, it would be highly irregular for a government agency to task the investigation of a fraud case to a civilian, non-governmental official.

25. According to Victim A, the scammers requested Victim A install a software program on his devices which allows a third-party remote access to a computer. Victim A indicated there were times when he could see someone "monitoring" his computer; for example, he could see someone remotely moving the cursor. The scammers also had Victim A leave a phone line "open" during the day so they could monitor activity. Victim A stated he would alternate between his cellular telephone and home phone number, in two-to-four-hour increments.[10] The scammers communicated with Victim A through what they described as a "secure line" hosted by Apple.[11]

26. According to Victim A, the scammers provided instructions to Victim A on how to make the money transfers. The scammers directed Victim A go to a local bank branch and initiate wire transfers to PeopleFirst Bank and Metropolitan Community Bank. The scammers told Victim A these banks had agreements with Crypto.com. The scammers provided details like bank address, account or routing number, and a reference or unique code. The scammers told Victim A they did not know who compromised his SSN so he needed to leave his cell phone on while visiting the branch

[10] According to Victim A, he was in telephone contact with the scammers from approximately 9:00 AM or 9:30 AM until 4:00 PM or 5:00 PM each day.

[11] The secure line, 425-588-0278, is assigned to a voice over IP telephone service. The subscriber records indicate the subscriber is "kush0895", not Apple. IP logs indicate the account was registered from an IP address in the Punjab state of India. This same VOIP telephone number was also provided to the FBI by the Evanston, Illinois victim, as one of the telephone numbers the scammers utilized.

so they (the scammers) could monitor for indictors of fraudulent behavior by the branch employees. The scammers assisted Victim A in setting up an account with Crypto.com, which included taking a photograph of himself sitting at his computer. The scammers directed Victim A to install Exodus, a digital currency wallet,[12] on his devices. Approximately 24 hours after sending the wire transfer, Victim A received an email from Crypto.com indicating the funds were available. The scammers then provided Victim A step-by-step instructions, via telephone, on how to make transfers, which included the use of the Crypto.com account to make transfers from Victim A's U.S. currency to cryptocurrency that, according to the scammers, would ultimately be deposited into the treasury accounts. The scammers told Victim A he had two treasury accounts: one for the funds that originated from his checking account and one for the funds that originated from his individual retirement account.

27. The scammers provided Victim A with documents entitled "confirmation letter" on bank letterhead which purport to show deposits into these treasury accounts. Victim A stated these confirmations reassured him everything was legitimate and is part of the reason he continued to engage with the scammers.

28. During an interview with Victim A, Victim A stated he followed the same procedures on behalf of funds belonging to his wife, Victim B.

29. During an interview with Victim A, Victim A stated he transferred between $3 and $4 million at the direction of the scammers. As described below, Victim

[12] Exodus wallet is a "self-custody" or non-custodial wallet, meaning the user of the wallet is acting as his/her own custodian of digital currency deposited in that wallet. The user accesses his/her wallet with a secret recovery phrase known as a seed phrase or a PIN code.

A's statement related to these transfers is corroborated by financial records obtained in the investigation.

30. According to publicly available information, Crypto.com is the "world's leading cryptocurrency platform" where users can "buy Bitcoin, Ethereum, and 250+ cryptocurrencies" and "trade with 20+ fiat currencies."[13] At the direction of the scammers, Victim A caused the following wire transfers to be sent from his traditional bank account held by a bank headquartered in Cherry Hill, New Jersey, to the Crypto.com correspondent bank (Metropolitan Commercial Bank) headquartered in New York:[14]

Date	Transfer Amount	Credit to Account
11/30/2022	$495,000.00	Victim A
12/08/2022	$495,000.00	Victim B
01/09/2023	$320,237.36	Victim A
03/09/2023[15]	$535,000.00	Victim A
03/17/2023[16]	$530,000.00	Victim B

[13] From https://crypto.com, last checked January 10, 2024.

[14] Based on SA Kadel's training and experience, bank wire transfers usually require the use of one or more interstate wire communications because the parties to the transaction, including the originator (in this case, the Victims), the originator's bank, the beneficiary bank, the beneficiary, and the processor—often the Federal Reserve Banks's Fedwire system—are typically geographically dispersed. In this case, the Victim was located in New Jersey, his bank was headquartered in New Jersey, and the receiving bank was located in New York. Additionally, Fedwire data centers are located in New Jersey and Texas, and transfers are processed in a multi-step process. As such, it is reasonable to believe some portion of the Victim's wire transfers affected interstate commerce and traveled interstate.

[15] This transfer was debited from Victim A's bank account on March 8, 2023 and posted to his Crypto.com account March 9, 2023.

[16] This transfer was debited from Victim A's bank account on March 16, 2023 and posted to his Crypto.com account March 17, 2023.

31. The FBI, through legal process, obtained account records from Crypto.com for an account owned by Victim A and an account owned by Victim B[17] and account records from Athena Bitcoin for an account owned by Victim A.[18] Victim A provided the FBI with a Microsoft Excel transaction history from his Exodus wallet which consists of both a Tether (USDT) address, **0x3fa26E,** and a Bitcoin address bc1qth95kp3d39rpytnu9dpluh8y3qrdw69xj24z5v (hereinafter **bc1qth95**). The FBI used these records, along with open-source analysis of the Bitcoin blockchain, and the Ethereum blockchain, to trace Victim A and Victim B's funds. In summary, the tracing shows approximately $784,940 of Victim A and Victim B's funds were transferred via intermediary addresses to the SUBJECT ASSETS and remained in the SUBJECT ASSETS at the time the addresses were frozen, on or about March 23, 2023.[19]

---

[17] Victim A stated both he and his wife opened accounts at Crypto.com at the direction of the scammers. Victim A stated he made all of the transfers on behalf of Victim B.

[18] According to publicly available information, Athena Bitcoin "is focused on developing, owning, and operating a global network of Athena-branded Bitcoin ATM machines" and "operates an over-the-counter ("OTC") desk known as ACE (Athena Crypto Exchange) for private clients and trade customers." *See* https://athenabitcoin.com/the-company/, last assessed January 10, 2024. According to Victim A, he transferred money to Athena Bitcoin at the direction of the scammers. Financial records obtained in the investigation corroborate Victim A's statement and indicate approximately $1,600,000 was transferred to Victim A's Athena Bitcoin account.

[19] The remaining funds were transferred through numerous digital currency addresses and co-mingled with funds from other known and unknown sources. For example, on February 6, 2023, 10 bitcoin and 156.933 ETH was transferred from Victim A's Athena Bitcoin account to Victim A's Exodus Wallet, converted to USDT (valued at approximately $475,784), then transferred to 0xAb5c360FB1B2802a51307452fd004429C6d3Eac9 (0xAb5c360F), an address controlled by an unknown person. Those funds were co-mingled in 0xAb5c360F with funds (approximately $4,303,447) transferred from 21 different addresses. Thereafter, the balance of 0xAb5c360F was depleted through a series of transfers (some round dollar, for example, $400,000) to addresses controlled by unknown person(s). These transfers are contrary to the representations the scammers made to Victim A (that his funds were being held in a "treasury account") and make traditional tracing techniques largely ineffective in locating the misappropriated funds and in the identification of the individual(s) in control of those funds. Based on SA Kadel's training and experience, and the facts and circumstances of this investigation, this type of conduct is consistent with money laundering.

32. Crypto.com account records show between November 30, 2022 and March 17, 2023, $2,375,237.36 was transferred from Victim A's bank account located at a United States-based financial institution headquartered in Cherry Hill, New Jersey to the Crypto.com correspondent account and credited to a Crypto.com customer account registered in Victim A's name or a Crypto.com customer account registered in Victim B's name.[20] Blockchain analysis[21] shows the money belonging to Victim A and Victim B was transferred out of the Crypto.com accounts as follows:

a. As detailed below, approximately 34,990 USDT from Victim A's Crypto.com account was transferred to Victim A's Exodus wallet and then to address **0x1bdd69 SUBJECT ASSET #1**.

i. On March 9, 2023, Victim A wired $535,000 to his Crypto.com account.

ii. On March 13, 2023, approximately $35,978 was converted to USDT.

iii. On March 13, 2023, approximately 34,990 USDT[22] was transferred from Victim A's Crypto.com account to his Exodus wallet, **0x3fa26E**.

iv. On March 14, 2023, 34,990 USDT was transferred from **0x3fa26E** to private address **0x1bdd69 SUBJECT ASSET #1.**

[20] Records obtained in this investigation indicate Victim A transferred approximately $2,375,237 to Crypto.com and approximately $1,660,000 to Athena Bitcoin, which is consistent with Victim A's statement that he transferred between $3 million and $4 million at the direction of the scammers.

[21] Unless otherwise noted, all dates and times referenced in the blockchain analysis are in UTC. All virtual asset amounts and USD conversion rate amounts are approximations.

[22] Records from Crypto.com indicate 35,000 USDT was transmitted but Victim A's Exodus Wallet transaction history and blockchain analysis indicate only 34,990 was transferred.

v. According to blockchain analysis, the balance of **0x1bdd69 SUBJECT ASSET #1** prior to this transaction was 0 USDT**.**

b. As detailed below, approximately 149,990 USDT was transferred from Victim B's Crypto.com account through a series of intermediary addresses to address **0x7c214b SUBJECT ASSET #2.**

i. On March 17, 2023, Victim A wired $530,000 to Victim B's Crypto.com account.

ii. On March 17, 2023, approximately $154,147 was converted to USDT.

iii. On March 17, 2023, approximately 149,990 USDT[23] was transferred from Victim B's Crypto.com account to private address 0x3baDab55546A6D117f4A72901D9c346bBb6b8F8C (hereinafter **0x3baDab**). This address is suspected to be the Exodus wallet address of Victim B.[24]

iv. On March 17, 2023, approximately 149,990 USDT was transferred from **0x3baDab** to private address

[23] Records from Crypto.com indicate 150,000 USDT was transmitted but blockchain analysis indicate only 149,990 was transferred.

[24] Victim A indicated he made transfers on behalf of his wife, Victim B, and that some of the same software (Exodus wallet) was installed on Victim B's phone. Victim A indicated Victim B's device had been cleaned and the wallet software was no longer available. Blockchain analysis indicates activity in the wallet began on December 8, 2022, which is around the time Victim A began engaging with the scammers. As such it is SA Kadel's belief that this address represents the private address in the Exodus wallet of Victim B.

0xD4A25F28D58130D78F548e89C4436f3b562cA34F (hereinafter **0xD4A25F INTERMEDIARY ADDRESS #1**).[25]

v. According to blockchain analysis, the balance of **0xD4A25F INTERMEDIARY ADDRESS #1** prior to this transaction was 0 USDT.

vi. On March 17, 2023, approximately 149,990 USDT was transferred from **0xD4A25F INTERMEDIARY ADDRESS #1** to **0x7c214b SUBJECT ASSET #2**.

vii. According to blockchain analysis, the balance of **0x7c214b SUBJECT ASSET #2** prior to this transaction was 0 USDT**.**

c. As detailed below, approximately 149,990 USDT was transferred from Victim A's Crypto.com account through a series of intermediary addresses to **0xcf95f2 SUBJECT ASSET #3**.

i. On March 9, 2023, the same day Victim A wired $535,000 to his Crypto.com account, approximately $153,917 was converted to USDT.

ii. On March 9, 2023, approximately 149,990 USDT was transferred from Victim A's Crypto.com account to his Exodus wallet, **0x3fa26E.**

iii. On March 9, 2023, approximately 149,990 USDT was transferred from **0x3fa26E** to **0xD4A25F INTERMEDIARY ADDRESS #1**.

[25] As described herein, **0xD4A25F** was utilized to transfer three discrete tranches of victim money. In each case, the balance of the address was 0 prior to the deposit of victim money, then fully liquidated.

iv. According to blockchain analysis, the balance of **0xD4A25F INTERMEDIARY ADDRESS #1** prior to this transaction was 0 USDT**.**

v. On March 9, 2023, approximately 149,990 USDT was transferred from **0xD4A25F INTERMEDIARY ADDRESS #1** to **0xcf95f2 SUBJECT ASSET #3**.

vi. According to blockchain analysis, the balance of **0xcf95f2 SUBJECT ASSET #3** prior to this transaction was 0 USDT**.**

d. As detailed below, approximately 149,990 USDT was transferred from Victim B's Crypto.com account to Victim B's suspected Exodus wallet to address **0xcf95f2 SUBJECT ASSET #3.**

i. On March 18, 2023, the day after Victim A wired $530,000 to Victim B's Crypto.com account, approximately $154,350 was converted to USDT.

ii. On March 18, 2023, approximately 149,990 USDT[26] was transferred from Victim B's Crypto.com account to Victim B's suspected Exodus wallet address, **0x3baDab**.

iii. On March 18, 2023, approximately 149,990 USDT was transferred from **0x3baDab** to **0xcf95f2 SUBJECT ASSET #3**.

[26] Records from Crypto.com indicate 150,000 USDT was transmitted but blockchain analysis indicate only 149,990 was transferred.

iv. According to blockchain analysis, the balance of **0xcf95f2 SUBJECT ASSET #3** prior to this transaction was 149,990 USDT, which are funds traceable to Victim A as described above**.**

e. As detailed below, approximately 149,990 USDT was transferred from Victim B's Crypto.com account to Victim B's suspected Exodus wallet to address **0xB8C348 SUBJECT ASSET #4.**

i. On March 20, 2023, three days after Victim A wired $530,000 to Victim B's Crypto.com account, approximately $154,188 was converted to USDT.

ii. On March 20, 2023, approximately 149,990 USDT[27] was transferred from Victim B's Crypto.com account to Victim B's suspected Exodus wallet address, **0x3baDab**.

iii. On March 20, 2023, approximately 149,990 USDT was transferred from **0x3baDab** to **0xB8C348 SUBJECT ASSET #4**.

iv. According to blockchain analysis, the balance of **0xB8C348 SUBJECT ASSET #4** prior to this transaction was 29,990 USDT**.** This 29,990 USDT can be traced to the Crypto.com account of Victim C.[28]

[27] Records from Crypto.com indicate 150,000 USDT was transmitted but blockchain analysis indicate only 149,990 was transferred.

[28] Victim C is an elderly resident of Richmond, Virginia and was interviewed by the FBI on multiple occasions. Initially Victim C denied being a victim of a scam. Subsequently Victim C realized he had been defrauded. In subsequent interviews, Victim C acknowledged he had been defrauded and described a scheme similar to the one described in this complaint. Victim C's total loss is unknown at this time, but believed to be several million dollars based on statements

f. As detailed below, approximately 149,990 USDT was transferred from Victim A's Crypto.com account through a series of intermediary addresses to address **0x9404a2 SUBJECT ASSET #5**.

i. On March 11, 2023, two days after Victim A wired $535,000 to his Crypto.com account, approximately $154,862 was converted to USDT.

ii. On March 11, 2023, approximately 149,990[29] USDT was transferred from Victim A's Crypto.com account to his Exodus wallet, **0x3fa26E**.

iii. On March 11, 2023, approximately 149,990 USDT was transferred from **0x3fa26E** to **0xD4A25F INTERMEDIARY ADDRESS #1.**

iv. According to blockchain analysis, the balance of **0xD4A25F** INTERMEDIARY ADDRESS #1 prior to this transaction was 0 USDT**.**

v. On March 12, 2023, approximately 299,980 USDT was transferred from **0xD4A25F INTERMEDIARY ADDRESS #1** to **0x9404a2 SUBJECT ASSET #5.**

vi. According to blockchain analysis, the balance of **0x9404a2 SUBJECT ASSET #5** prior to this transaction was 0 USDT**.** The amount of this transfer consists of 149,990 USDT belonging to

made to the FBI by Victim C and his associates and based on preliminary analysis of financial records obtained in the investigation.

[29] Records from Crypto.com indicate 150,000 USDT was transmitted but blockchain analysis indicate only 149,990 was transferred.

Victim A, as described above, and 149,990 USDT traced to the Crypto.com address of Victim C.

33. Below is a table summarizing the tracing of Victim A and Victim B funds into the SUBJECT ASSETS at the time the accounts were frozen, on or about March 23, 2023:

Address	USDT	USD Equivalent (Approximate)
0x1bdd69	**34,990**	$34,990
0x7c214b	**149,990**	$149,990
0xcf95f2	**299,980**	$299,980
0x9404a2	**149,990**	$149,990
0xB8C348	**149,990**	$149,990

34. Legal process was issued to Tether requesting information about the user(s) of **0x1bdd69**, **0x7c214b**, **0xcf95f2**, **0xB8C348**, and **0x9404a2** (the SUBJECT ASSETS). Tether responded to the legal process indicating it did not have any information about the person(s) utilizing the addresses.[30] At the request of law enforcement, on or around March 23, 2023, Tether temporarily restrained the assets in **0x1bdd69**, **0x7c214b**, **0xcf95f2**, **0xB8C348**, and **0x9404a2** (the SUBJECT ASSETS). This process blocks the transfer of funds out of the addresses but allows for deposits into the addresses.

35. According to blockchain analysis, **0x1bdd69 SUBJECT ASSET #1** has been active since December 20, 2022. Between December 20, 2022 and March 2, 2023, **0x1bdd69** received three deposits totaling 246,973 USDT and sent four withdrawals

[30] According to the Tether response, the addresses are not owned or controlled by Tether and open source software can be used by any person to generate and uses addresses for transfers without involvement by Tether.

totaling 246,973 USDT. As of March 23, 2023, the balance in **0x1bdd69** was 34,990 USDT. As of February 23, 2024 (the date of the seizure warrant), the balance was 34,990 USDT. As noted above, on March 6, 2024 the assets were "burned" from the subject addresses and reissued to government controlled addresses.

36. According to blockchain analysis, **0x7c214b SUBJECT ASSET #2** has been active since February 28, 2023. Between February 28, 2023 and March 2, 2023, **0x7c214b** received one deposit in the amount of 367,200 USDT and sent one withdrawal in the amount of 367,200 USDT. On March 17, 2023, **0x7c214b SUBJECT ASSET #2** received a deposit in the amount of 149,990 USDT, traced to Victim B's suspected Exodus wallet address, as detailed above. As of March 23, 2023, the balance in **0x7c214b** was 149,990 USDT. As of February 23, 2024, the balance was 149,990 USDT.

37. According to blockchain analysis, **0xcf95f2 SUBJECT ASSET #3** has been active since October 31, 2022. Between October 31, 2022 and March 2, 2023, **0xcf95f2 SUBJECT ASSET #3** received seven deposits totaling 572,719 USDT and sent six withdrawals totaling 572,719 USDT. On March 9, 2023, **0xcf95f2 SUBJECT ASSET #3** received a deposit in the amount of 149,990 USDT traced to Victim A, detailed above. On March 18, 2023, **0xcf95f2 SUBJECT ASSET #3** received a deposit in the amount of 149,990 USDT from Victim B, detailed above. As of March 23, 2023, the balance in **0xcf95f2 SUBJECT ASSET #3** was 299,980 USDT. Since then, **0xcf95f2 SUBJECT ASSET #3** received three deposits totaling 320,104 USDT.[31] As of February 23, 2024, the balance was 620,084 USDT.

[31]149,990 USDT was deposited on March 25, 2023 from private wallet address 0xb9C31e997DB9D7CB94A9FCB4d27526c3B4A44767. Through legal process, the FBI traced

38. According to blockchain analysis, **0xB8C348 SUBJECT ASSET #4** has been active since December 20, 2022. Between December 20, 2022 and March 2, 2023, **0xB8C348 SUBJECT ASSET #4** received three deposits totaling 268,557 USDT and sent three withdrawals totaling 268,557 USDT. On March 14, 2023, **0xB8C348 SUBJECT ASSET #4** received a deposit in the amount of 29,990 USDT traced to the Crypto.com account of Victim C as detailed above. On March 20, 2023, **0xB8C348 SUBJECT ASSET #4** received a deposit in the amount of 149,990 USDT from Victim B as detailed above. As of March 23, 2023, the balance in **0xB8C348 SUBJECT ASSET #4** was 179,980 USDT. As of February 23, 2024, the balance was 179,980 USDT.

39. According to blockchain analysis, **0x9404a2 SUBJECT ASSET #5** has been active since November 26, 2022. Between November 26, 2022 and March 2, 2023, **0x9404a2 SUBJECT ASSET #5** received six deposits totaling 751,026 USDT and sent three withdrawals totaling 751,026 USDT. On March 12, 2023, **0x9404a2 SUBJECT ASSET #5** received a deposit in the amount of 299,980 USDT from **0xD4A25F INTERMEDIARY ADDRESS #1**. These funds were traced to Victim A and Victim C, as detailed below. As of March 23, 2023, the balance in **0x9404a2 SUBJECT ASSET #5** was 299,980 USDT. On March 28, 2023, **0x9404a2 SUBJECT ASSET #5** received a

---

these funds to the Crypto.com account of Victim D. Victim D is an elderly resident of Ocala, Florida and was interviewed by SA Kadel. According to Victim D, she was defrauded in a scheme similar to the one described in this complaint. Victim D's total loss, based on statements to the FBI and blockchain analysis, is estimated to be approximately $930,000. 170,014 USDT was deposited on March 28, 2023 from private wallet address 0xA333Ff74631b348733B8ef8047D684E6210bF0ee. 100 USDT was deposited on May 3, 2023 from private wallet address 0x563a305E9a57e8e8aC33BAf4fF92dAF67F603dE5. As of the date of this complaint, the individual(s) who sent these funds have not been identified.

deposit in the amount of 149,990 USDT.[32] As of February 23, 2024, the balance was 449,970 USDT.

40. According to blockchain analysis, **0xD4A25F INTERMEDIARY ADDRESS #**1 has been active since February 24, 2023. Between February 24, 2023 and March 17, 2023, **0xD4A25F INTERMEDIARY ADDRESS #1** received fifteen (15) deposits totaling 2,441,949 USDT and sent thirteen (13) withdrawals totaling 2,441,949 USDT. As of March 23, 2023, the balance in **0xD4A25F INTERMEDIARY ADDRESS #1** was 0 USDT. On March 11, 2023, **INTERMEDIARY ADDRESS #1** received a deposit of 149,990 USDT from the Exodus wallet of Victim A (**0x3fa26E**). According to blockchain analysis, the balance of **0xD4A25F INTERMEDIARY ADDRESS #1** prior to this transaction was 0 USDT.

41. According to blockchain analysis, also on March 11, 2023, **0xD4A25F INTERMEDIARY ADDRESS #1** received a deposit of 149,990 USDT from Victim C. According to blockchain analysis, after this transfer the balance in **0xD4A25F INTERMEDIARY ADDRESS #1** was 299,980 USDT. On March 12, 2023, 299,980 USDT was transferred from **0xD4A25F INTERMEDIARY ADDRESS #1** to **0x9404a SUBJECT ASSET #5**.

[32]149,990 USDT was deposited on March 28, 2023 from private address 0x97F51d5EB6B6244ee31c5ffB0a13F3cbe390B8FC. Through legal process, the FBI traced these funds to the Crypto.com account of Victim E. Victim E is an elderly resident of La Quinta, California and was interviewed by SA Kadel. According to Victim E, he was defrauded in a scheme similar to the one described in this complaint. Victim E's total loss, based on statements to the FBI and blockchain analysis, is estimated to be approximately $645,000.

WARRANT FOR ARREST IN REM

42. Upon the filing of this complaint, the plaintiff requests that the Court issue an arrest warrant in rem pursuant to Supplemental Rule G(3)(b), which the plaintiff will execute upon the defendant property pursuant to 28 U.S.C. § 1355(d) and Supplemental Rule G(3)(c).

CLAIM FOR RELIEF

43. The plaintiff repeats and incorporates by reference the paragraphs above.

44. By the foregoing and other acts, the defendant property constitutes or was derived from proceeds traceable to specified unlawful activity, namely, wire fraud, committed in violation of 18 U.S.C. § 1343, and is therefore subject to forfeiture to the United States of America under 18 U.S.C. § 981(a)(1)(C) with cross-references to 18 U.S.C. §§ 1956(c)(7) and 1961(1).

45. By the foregoing and other acts, the defendant property was involved in, or is traceable to funds involved in, money laundering transactions in violation of 18 U.S.C. §§ 1956 and 1957 and is therefore subject to forfeiture to the United States of America under 18 U.S.C. § 981(a)(1)(A).

WHEREFORE, the United States of America requests:

a. the defendant property be proceeded against for forfeiture and condemnation;

b. due notice be given to all interested parties to appear and show cause why the forfeiture should not be decreed; and

c. this court adjudge and decree that the defendant property be forfeited to the United States and disposed of according to law.

Respectfully submitted,

MORRIS PASQUAL
Acting United States Attorney

By: */s/ Steven Dollear*

STEVEN DOLLEAR
Assistant United States Attorney
219 South Dearborn Street
Chicago, Illinois 60604
(312) 353-5300

VERIFICATION

1. I, Jayna Kadel, hereby verify and declare under penalty of perjury, that I am a Special Agent with the Federal Bureau of Investigation and have been so employed since approximately 2014. As part of my duties as an FBI Special Agent, I investigate criminal violations relating to white collar crimes, including mail, wire, and bank fraud. In addition, I have received training on how people use computers to commit crimes and the law enforcement techniques that can be used to investigate and disrupt such activity. I have participated in federal search and seizure warrants to include warrants pertaining to the seizure of digital information and digital assets.

2. I have read the foregoing Verified Complaint in this matter and the facts alleged are true and correct to the best of my knowledge and belief based upon my own personal knowledge as well as information I have received from other agents, persons and documents, and it does not include each and every fact known to me concerning this investigation.

I hereby verify under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 5th day of December 2024.

Jayna Kadel

Jayna Kadel
Special Agent
Federal Bureau of Investigation